Sourcegraph

Why Sourcegraph's single-tenant cloud instance is the most secure way to deploy Sourcegraph

Last updated August 15, 2023

1. Better security protections than companies typically implement for internal, self-hosted tools

Sourcegraph Cloud is SOC 2 Type II audited and regularly pen tested by independent auditors. Customer data is encrypted at rest and in transit and backed-up daily. Any infrastructure change must pass security checks, which are tested against industry standard controls.

In addition, Sourcegraph continuously monitors cloud instances for security issues, using manual reviews and automated tools. Cloud instances are fully managed by a dedicated team of Sourcegraph experts who maintain 24/7 incident response.

Most companies cannot say the same for their internal, self-hosted tools.

2. Automatic updates that fix vulnerabilities

Cloud instances are automatically upgraded to fix any vulnerability in third-party dependencies. In addition, GCP's managed offering regularly patches any vulnerability in the underlying infrastructure.

Self-hosted instances, to the contrary, require customers to manually update the version. As a result, many self-hosted customers remain on outdated versions, resulting in a less secure and buggier experience.

3. Dedicated infrastructure that prevents security and performance concerns of shared infrastructure

Unlike many cloud services, Sourcegraph Cloud is single-tenant rather than multi-tenant, thus removing risks of cross-tenant security breaches. Each customer's data is secured in a dedicated, fully segregated GCP project. This structure offers maximum security and state-of-the-art isolation, making Sourcegraph Cloud more secure and reliable than self-hosting Sourcegraph in a shared infrastructure. Sourcegraph Cloud can also be hosted in any GCP region, meeting customers' data sovereignty requirements.